

Memorandum

U.S. Department
of Transportation
**Federal Aviation
Administration**

Subject: INFORMATION: Policy Statement on Guidance for
Determination of System, Hardware, and Software
Development Assurance Levels on Transport Category
Airplanes

Date: January 15, 2004

From: Acting Manager, Transport Airplane Directorate, Aircraft
Certification Service, ANM-100

Reply to
Attn. of: ANM-03-117-09

To: See Distribution

Regulatory §§ 25.1301 and
Reference: 25.1309; AC 25.1309-
1A, and AC 20-115B

Summary

The purpose of this memorandum is to clarify Federal Aviation Administration (FAA) Transport Airplane Directorate (TAD) certification policy on determination of system development assurance levels, hardware design assurance levels, and software levels.

Current Regulatory and Advisory Material

1. Advisory Circular (AC) 20-115B.
2. Section 25.1301 of Title 14 Code of Federal Regulations (CFR) Part 25.
3. Section 25.1309 of 14 CFR Part 25.
4. Advisory Circular 25.1309-1A.
5. Society of Automotive Engineers (SAE) Aerospace Recommended Practice ARP4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems, issued 1996-11.
6. Society of Automotive Engineers ARP4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment, issued 1996-12.
7. Radio Technical Commission for Aeronautics (RTCA) DO-254, Design Assurance Guidance for Airborne Electronic Hardware, issued April 19, 2000.
8. Radio Technical Commission for Aeronautics DO-178B, Software Considerations in Airborne Systems and Equipment Certification, issued December 1, 1992.

Relevant Past Practice

Failure analysis and design validation and verification have traditionally been accomplished with extensive tests conducted on the system and its components, direct inspection, and other direct verification methods capable of correctly characterizing the operations of the system. These direct techniques are still appropriate for simple systems which perform a limited number of functions and which are not highly integrated with other aircraft systems. For more complex or integrated systems, adequate testing may either be impossible because all of the system states cannot be determined or it may be impractical due to the large number of tests which must be accomplished.

The regulations and policy applicable to the subject of design/development assurance level assignment are §§ 25.1301 and 25.1309, currently at Amendment 25-42, and Advisory Circular (AC) 25.1309-1A. Advisory Circular 20-115B recognizes that the guidelines of RTCA DO-178B may be used to develop software used in digital electronics for airborne applications.

The Aviation Rulemaking Advisory Committee (ARAC) has recommended harmonized FAR/JAR 25.1301 and 25.1309, and associated advisory material. A section of the recommended AC recognizes the use of system architecture, as described in SAE ARP 4754, as an acceptable means to determine system, hardware, and software levels and that where apparent differences exist between these documents on this subject, the guidance contained in Appendix D of SAE ARP4754 can be followed. Advisory Circular 23.1309-1C (paragraph 12) adopted a similar position for small airplanes.

The FAA has not formally recognized RTCA DO-254 (with an AC) as of this writing, although the TAD has issued several issue papers on various certification programs that recognize RTCA DO-254 as an acceptable means of compliance for programmed logic devices (PLD) that is currently applied to all part 25 airplanes and system programs.

Guidelines for the development of airborne systems, software, and electronic hardware components, are contained in SAE ARP4754, RTCA DO-178B, and RTCA DO-254, respectively. Because these documents were not developed simultaneously, they contain different guidance and terminology. For ease and readability, please note that Development Assurance Level (DAL), Design Assurance Level (DAL), and Software Level (SL) are used synonymously within this memorandum.

A significant difference between the SAE ARP4754 and RTCA DO-178B is the guidance provided on the use of system architecture for determining the appropriate DALs for hardware and software. The FAA recognizes that consideration of system architecture for the purpose of establishing DALs is appropriate. A seamless transition between these guidelines has not been clearly established to guide the determination of system, software, and hardware DALs. Until such time, the policy below provides a standardized approach to the use and application of these guidelines and industry practices.

Policy

1. As the development assurance level determination is inherently a key process step in airplane and system safety assessment, the Aircraft Certification Office (ACO) Aviation Safety Engineer (ASE) (or authorized designee) should confirm that the airplane level functional hazard assessment (FHA), the system level FHA, and the preliminary system safety assessment (PSSA) are correctly performed (effects of loss of function as well as malfunction should be evaluated), and that the PSSA contains proposals for DALs for the system and each of its software and hardware items. Applicants should be encouraged to submit these safety assessments to the FAA for approval early in the program in order to minimize certification risks.
2. System, hardware, and software DALs may be assigned based on a direct relationship to the worst-case failure condition; namely, Catastrophic corresponds to Level A, Hazardous/Severe-Major to Level B, Major to Level C, Minor to Level D, and No Safety Effect to Level E. This method, particularly when applied to a system architecture with redundant elements, may result in a more conservative assignment of the DALs to the redundant elements than is necessary to comply with §§ 25.1301 and 25.1309. However, any reduction in DAL from the levels determined by this method should be presented, with justification, to the ACO ASE early in the program for approval.
3. If a design could contain common mode design errors that could be catastrophic, the applicable software and hardware should be assigned Level A. The software and hardware DALs could potentially be reduced as justified by the safety assessment if the system architecture is revised to mitigate the potential catastrophic condition.
4. The guidance of SAE ARP4754 may be used to assign DALs for a system and its hardware and software components. When application of this guidance leads to assignments of DALs lower than those determined using the direct assignment of policy 2 above, the applicant should obtain concurrence of the cognizant FAA ACO with the results of the proposed PSSA as early as possible in the program in order to minimize certification risks. If the criteria of the SAE ARP4754 are not satisfied, the DALs may need to be assigned a higher level using the direct assignments of policy 2 above or using the guidance of RTCA DO-178B.
5. The guidance of RTCA DO-178B has traditionally been used and may continue to be used in the PSSA, as appropriate, to determine software levels. Where apparent differences exist between RTCA DO-178B and SAE ARP4754 on software level determination, the guidance contained in Appendix D of SAE ARP4754 can be used if additional credit is requested for system architecture and justification is provided to the cognizant ACO for concurrence.

6. For transport category airplanes, RTCA DO-254 is applicable to all electrical and electronic devices whose correct operation cannot be verified by test and/or deterministic analysis if they could cause Major, Severe Major/Hazardous, and Catastrophic failure conditions.

EFFECT OF POLICY

The general policy stated in this document does not constitute a new regulation or create what the courts refer to as a "binding norm". The office that implements policy should follow this policy when applicable to the specific project. Whenever an applicant's proposed method of compliance is outside this established policy, it must be coordinated with the policy issuing office, e.g., through the issue paper process or equivalent. Similarly, although this policy is not binding on the FAA, if the implementing office becomes aware of reasons that an applicant's proposal that meet this policy should not be approved, the office must coordinate its response with the policy issuing office.

Applicants should expect that the certificating officials will consider this information when making findings of compliance relevant to new certificate actions. Also, as with all advisory material, this policy statement identifies one means, but not the only means, of compliance.

Additional detail is provided in the Appendix as well as tutorial examples to aid in the understanding of the policy contained herein.

Questions and comments regarding this policy should be directed to the Transport Standards Staff, Safety Management Branch, ANM-117, c/o Mr. Linh Le, email linh.le@faa.gov, phone 425-227-1105, fax 425-227-1100.

/s/

Ali Bahrami

APPENDIX

A. THE ISSUES

There have been some inconsistencies in determining the system development assurance levels, hardware design assurance levels, and software levels (collectively referred to as “DAL” from this point forward for ease of readability) in the past using the guidelines contained in SAE ARP4754, RTCA DO-254, and RTCA DO-178B, respectively.

- Although system safety assessment is the common input, SAE ARP4754 and RTCA DO-178B can recommend different software levels in certain circumstances. There are some opinions that SAE ARP4754 is not sufficiently conservative compared to RTCA DO-178B when software levels are determined. Although SAE ARP4754 has been acknowledged by ARAC as stated above, the issue persists because the TAD has not published a formal recognition of its use on transport category airplanes.
- Radio Technical Commission for Aeronautics DO-178B uses the clause “cause or contribute to a failure of system function” when defining software level (reference section 2.2.2). The term “contribute” is often interpreted as recommending the software level associated with system malfunctioning rather than just loss of system function, regardless of the system architecture. This interpretation has at times led to a more conservative assignment of software level than is needed to meet the regulation.
- In addition, RTCA DO-254 has recently been published, and it contains recommendations for electronic hardware design assurance levels. The application of RTCA DO-254 to part 25 avionics hardware needs to be defined in a manner that is consistent with the application of SAE ARP4754 and RTCA DO-178B.

B. POLICY DERIVATION

(1) Main Differences between the Guidelines:

- Scope:
Radio Technical Commission for Aeronautics DO-178B was primarily developed to address the “software aspects of certification” and described guidelines to achieve the objectives established for the different software levels. It was not intended to be guidance for system nor hardware development. Further, RTCA DO-178B was developed based on the federated system architecture perspective, and it did not include considerations for highly integrated, complex systems.

Society of Automobile Engineers ARP4754 was developed from the perspective of complex or highly integrated systems. It excludes specific coverage criteria for validation and verification processes for software and hardware. It only covers those aspects that are of significance in establishing the safety of a system. However, it contains examples of DAL assignments to system as well as hardware and software. The philosophy behind its DAL assignments is not always congruent with that of DO-

178B.

- Radio Technical Commission for Aeronautics DO-254 provides design assurance guidance for airborne electronic hardware. It does not provide guidance for software and system development. It provides guidelines for conducting a hardware safety assessment which includes methods for selecting appropriate design strategies for electronic hardware that vary based on the hardware design assurance level assigned. The hardware safety assessment, the functional hazard assessment (FHA), the preliminary system safety assessment (PSSA), a technique called Functional Failure Path Analysis, and, as time permits, the system safety assessment (SSA) processes are used in combination to determine hardware DALs.
- Degree of Rigor:
Society of Automotive Engineers ARP4754 and RTCA DO-254 both assign Level “A” to systems and hardware that cause catastrophic failure conditions and Level “B” for hazardous/severe major failure conditions, but in general there is little difference in the amount of rigor (validation, verification, etc.) between these two levels. [Perhaps the most noticeable difference between Levels A and B in SAE ARP4754 is the quantitative safety objectives, 10^{-9} versus 10^{-7} (reference Table 6). In RTCA DO-254, Level A differs from B in that it *may* require more “design assurance strategies” to provide more complete mitigation of failures and anomalous behaviors (reference step 4 of Figure 2.3 of RTCA DO-254).]

In RTCA DO-178B, the difference between Level A and B is that Level A requires more rigorous exercising of the code structure (modified condition/decision coverage) versus decision coverage for Level B; and Level A also requires more verification independence than Level B.

(2) Application Examples

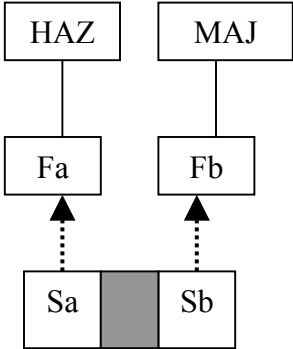
The following examples illustrate the DAL assignment as recommended by SAE ARP4754, RTCA DO-178B, and RTCA DO-254, for a number of example system architectures. The examples herein are not all inclusive, as practical system designs have a wide range of architectures that do not perfectly match these example architectures. The examples are intended to highlight the differences and similarities between the guidelines, to provide background information for the policy established in this memorandum, and to provide tutorial for the use of the policy.

Examples 1 through 5 take the architectures presented in Table 4 of SAE ARP4754 section 5.4, as the baseline to study the DAL assignment methods using the guidance in SAE ARP4754, RTCA DO-178B and RTCA DO-254. Examples 6 and 7 employ more “realistic” system architectures. In each case, it is assumed that the FHA and PSSA have been correctly performed. Since the PSSA already considers mitigation factors such as independence, redundancy, dissimilarity, partitioning, monitoring, flightcrew and maintenance actions, etc., for brevity such factors are not discussed in the examples.

It should be noted that DAL assignment is one of the last steps in the PSSA process, and that SAE ARP4761 recognizes SAE ARP4754 for DAL assignments if system architecture is to be considered (reference section D.10.4). While the examples illustrate the differences between the guidance recommendations, given the same safety

assessment results, they are not intended to illustrate how the FHA/PSSA should be done. See SAE ARP4761, Appendix B, for details of the PSSA process, and Appendix D.12 for qualitative guidance on using fault trees to show contribution of design errors.

EXAMPLE 1a: Partitioned Design (Reference SAE ARP4754, section 5.4.1.1, and RTCA DO-178B, section 2.3.1)

Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
 <p>Fa and Fb are independent functions that are implemented by systems Sa and Sb, respectively. Sa and Sb are partitioned.</p> <p>Suppose the safety assessment are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> ▪ Effects of Fa alone: Hazardous ▪ Effects of Fb alone: Major ▪ Both functions fail: Hazardous <p>PSSA:</p> <ul style="list-style-type: none"> ▪ Failure of one function can not impact the other. ▪ Dissimilar hardware in Sa and Sb 	<p>Per item 1 in Table 4:</p> <p>Level B for the overall system including establishment of the partition.</p> <p>The DALs for Sa and Sb correlate to their individual failure effects:</p> <p>Sa is Level B associated to its Hazardous effect.</p> <p>Sb is Level C corresponding to the Major effect.</p>	<p>If the functions Fa and Fb are implemented in software, then per section 2.3.1 Partitioning:</p> <p>Software in Sa is Level B because the most severe effect of Fa is Hazardous.</p> <p>Software in Sb is Level C corresponding to its Major effect.</p> <p>If the partitioning protection involves software, then per 2.3.1.c that software is Level B corresponding to the highest level of the <u>partitioned software components</u>.</p>	<p>Function Fa is at Level B because its worst effect is Hazardous, so the hardware in Sa is Level B.</p> <p>Function Fb is at Level C because its worst effect is Major, so the hardware in Sb is Level C.</p> <p>Per 2.3.1 the partitioning protection would be Level B.</p>

Summary

The three guidelines assign the same DALs, and the assignments are consistent with the “direct” method of policy 2.

EXAMPLE 1b: Partitioned Design (Reference SAE ARP4754, section 5.4.1.1 and 5.4.1.4, and RTCA DO-178B, section 2.2.3 and 2.3.1)

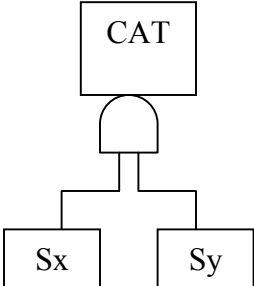
Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
<p>Multiple a/c level functions implemented on common hardware.</p> <p>Channel 1</p> <p>Channel 2</p> <p>Fa and Fb are independent functions representing an active command and a monitor that are implemented by systems Sa and Sb, respectively. Sa and Sb are integrated in a computer system that provides the multiple functions from two <u>identical</u> channels.</p> <p>Suppose the safety assessment results are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> Failure (undetected malfunction) of <u>both</u> functions Fa and Fb is Catastrophic. Fa alone (loss of function): Major Fb alone (loss of function): Major <p>PSSA:</p> <ul style="list-style-type: none"> DAL for Sa to be higher than Sb's DAL. Failure of Channel 1: Major Failure of Channel 2: Major 	<p>Per item 1 and 4 in Table 4:</p> <p>The overall system is Level A including the establishment of the partition.</p> <p>Either Sa or Sb is raised to Level A per section 5.4.1.4. In this example the PSSA assigned the higher Level to Sa. Therefore Sa (1 and 2) is Level A and Sb (1 and 2) is Level C.</p> <p>Per Note 2 of table, the switching, voting, fault detection would be Level A.</p>	<p>If the functions Fa and Fb are implemented in software, then per section 2.2.3, the software is Level A for at least one system, because it contributes to a Catastrophic failure condition.</p> <p>Per section 2.3.1 Partitioning: Software in Sa (1 and 2) is Level A as assigned by the PSSA. Software in Sb (1 and 2) is Level C corresponding to its Major category.</p> <p>If the partitioning protection involves software, then per 2.3.1.c that software is Level A corresponding to the highest level of the <u>partitioned software components</u>.</p>	<p>Since the common hardware is used to implement Sa and Sb, the hardware design assurance Level is A to accommodate the PSSA assignment of Level A to Sa.</p>

Summary

- The software levels are consistent between SAE ARP4754 and RTCA DO-178B as guided by the PSSA.
- Since both Fa and Fb “contribute” to the catastrophic top event, it could be construed that Sa and Sb software should be Level A. However, the redundancy, independence and partitioning protection provides the architectural mitigation means that allows Sb to be Level C.
- The hardware DAL assigned by RTCA DO-254 is higher for Sb than SAE ARP4754 recommends because of the potential for common hardware failure. The FAA recommends that alternative means to mitigate the common faults should be evaluated. However, if

changing the architecture to achieve dissimilar designs were determined to be impracticable, Level A DAL would be needed.

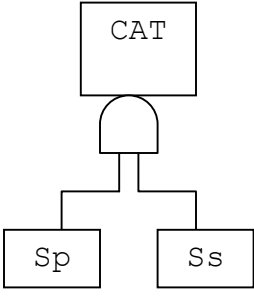
EXAMPLE 2: Parallel Architecture – Dissimilar-and-Independent Designs
Implementing an Airplane-Level Function (Reference SAE ARP4754, section 5.4.1.2, and RTCA DO-178B, sections 2.2.3, 2.3.1 and 2.3.2)

Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
<p>An a/c level function is implemented in a parallel architecture with the attributes described in SAE ARP4754 section 5.4.1.2 (also see examples in Footnote 2 on page 28 of SAE ARP4754.)</p>  <pre> graph TD CAT[CAT] --- AND[AND] AND --- Sx[Sx] AND --- Sy[Sy] </pre> <p>Parallel systems Sx and Sy provide for the a/c level function and they are <u>dissimilar and independent</u>.</p> <p>Suppose the safety assessment findings are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> ▪ Effects of function failures: <ul style="list-style-type: none"> ▪ Malfunction = Catastrophic ▪ Loss = Major ▪ Effect of Sx alone: Major ▪ Effect of Sy alone: Major <p>PSSA:</p> <ul style="list-style-type: none"> ▪ No hardware common mode failures ▪ The "independent and dissimilar" criteria are met; i.e., the architecture satisfies the design assurance objectives (for example, the architecture provides the risk mitigation even without MC/DC.) 	<p>Per item 2 in Table 4 of SAE ARP4754:</p> <p>The overall system is Level A. Sx and Sy are Level B (provided dissimilarity and independence are rigorously validated and verified).</p> <p>Per Note 2 of table, any switching, voting, fault detection would be Level A.</p>	<p>Using the guidance of section 2.2.3, if software is used in Sx and Sy, at least one is software Level A. The other may be Level C associated with the <u>loss</u> of the aircraft level function. The PSSA would specify which system to have Level A and which would have Level C.</p> <p>If implemented in software, the failure detection/monitoring/switching logic is Level A.</p>	<p>Although there may be cases where it might be possible to justify level C for both Sx and Sy, this example will assume the PSSA uses the strategy contained in SAE ARP4754 for DAL assignment, Level B would be assigned to the hardware of Sx and Sy.</p>

Summary

- Application of the policy would result in the component DALs to be Level B, although the overall system requirement is still Level A. Note the built-in conservatism, as the DALs are higher than those associated with the individual system effects.
- The software levels resulting from the SAE ARP4754 recommendations (B and B) are different from the software levels recommended by RTAC DO-178B (A and C). The policy of this Memorandum would assign Level B initially to both software components, based on the system architecture.

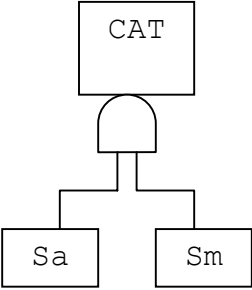
EXAMPLE 3: Parallel Architecture – Redundant-channel System Design Implementing an Airplane-Level Function (Reference SAE ARP4754, section 5.4.1.3, and RTCA DO-178B, section 2.2.3)

Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
<p>An a/c level function is implemented in a parallel architecture with redundant channels as described in SAE ARP4754, section 5.4.1.3.</p>  <p>Primary channel Sp and secondary channel Ss provide an a/c level function. Sp is always used unless it has failed. Ss does not contribute to fault detection, and cannot cause Sp to fail.</p> <p>Suppose the safety assessment findings are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> ▪ Effects of combined failure: <ul style="list-style-type: none"> ▪ Malfunction = Catastrophic ▪ Loss = Major ▪ Effect of Sp alone: Major ▪ Effect of Ss alone: Major <p>PSSA:</p> <ul style="list-style-type: none"> ▪ Sp is a different design from Ss ▪ The failure rate of Sp must be less than 1×10^{-5} per paragraph 5.4.1.3 of SAE ARP4754. 	<p>Per item 3 in Table 4:</p> <p>The overall system is Level A. The primary portion Sp is Level A, and the secondary portion Ss is Level B regardless of their individual failure effect.</p> <p>The failure detection/monitoring/switching logic is Level A per Note 2 of the Table.</p>	<p>The guidance for parallel implementation Section 2.2.3 recommends the software in either Sp or Ss is at Level A while the other can be Level C associated with <u>loss</u> of the aircraft level function. The PSSA would specify which system would be assigned Level A and which would have Level C.</p> <p>If implemented in software, the failure detection/monitoring/switching logic is Level A.</p>	<p>For the purpose of this example, the PSSA uses the same strategy as SAE ARP4754 to assign Level A to the hardware in Sp and Level B to Ss.</p>

Summary

- The most notable difference is RTCA DO-178B assigns Level C to the software for one of the channels where SAE ARP4754 assigns Level B to the Ss software and its associated system and hardware. The policy of this Memorandum would initially result in Level B for that software to be consistent with its system and hardware DAL assignments. (Note: there may be circumstances where a lower criticality application software is loaded on a “high DAL” hardware.)

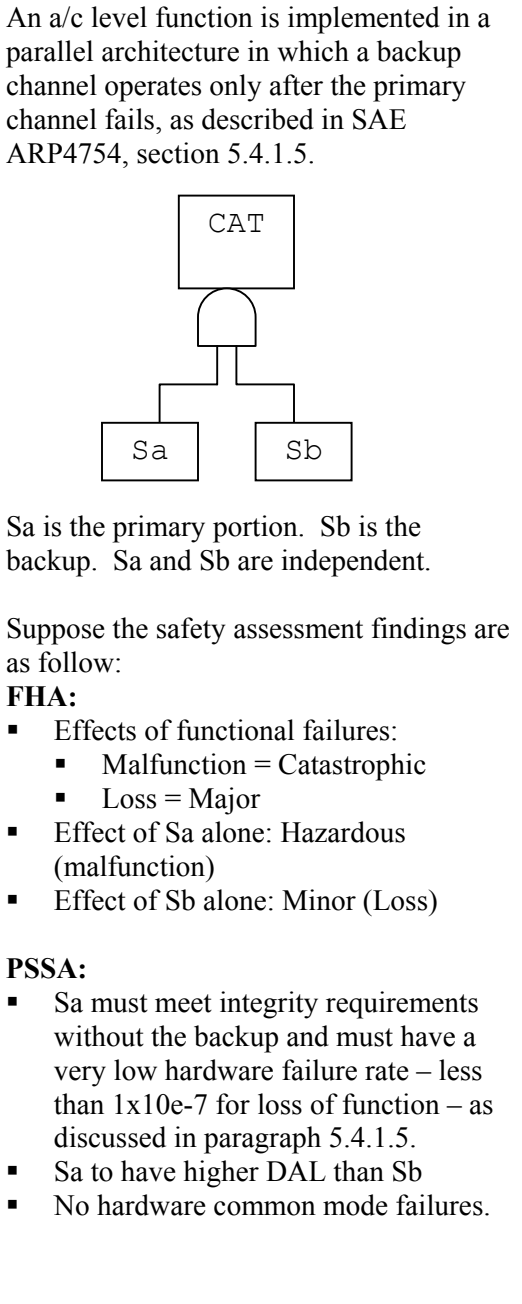
EXAMPLE 4: Active-Monitor Parallel Architecture (Reference SAE ARP4754, section 5.4.1.4, and RTAC DO-178B, section 2.3.3) with Dissimilar Hardware

Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
<p>An a/c level function is implemented in a parallel architecture where a monitor is needed to meet the integrity requirement, as described in SAE ARP4754, section 5.4.1.4.</p>  <p>Sa is the active portion. Sm is the monitor. Sm and Sa are independent.</p> <p>Suppose the safety assessment findings are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> ▪ Effects of failures: <ul style="list-style-type: none"> ▪ Malfunction = Catastrophic ▪ Loss = Major ▪ Effect of Sa alone: <ul style="list-style-type: none"> ▪ Malfunction = Major (would be Catastrophic without the monitor) ▪ Loss = Major ▪ Effect of Sm alone: <ul style="list-style-type: none"> ▪ Malfunction (nuisance shutdown) = Major ▪ Loss (always indicates system is operating normally) = Major <p>PSSA:</p> <ul style="list-style-type: none"> ▪ No hardware common mode failures ▪ The monitor detects all failures 	<p>Per item 4 in table 4:</p> <p>The overall system is Level A.</p> <p>Regardless of their individual effects, either Sa or Sm can be Level A. If Sa is Level A, then Sm can be Level C. If Sm is Level A, then Sa is Level C.</p> <p>Per Note 2 of the table, the switching, voting, fault detection is Level A.</p>	<p>Per 2.3.3 Safety-Monitoring:</p> <p>The s/w in Sa can be lowered to the level associated with <u>loss</u> of a/c function (C in this case) provided Sm s/w has the following three attributes:</p> <ol style="list-style-type: none"> 1) it is developed to Level A, 2) it has adequate fault coverage, 3) it is independent from Sa. 	<p>For the purpose of this example, the same strategy as SAE ARP4754 is used to assign Level A to the hardware of Sa and Level C to the hardware of Sm. Alternatively, Level C could be used for Sa and Level A for Sm.</p>

Summary

- If the PSSA requires Level A for the active portion, application of the policy would allow the monitor software to be Level C. If the PSSA selects Level A for the monitor portion, then the active portion can be Level C.

EXAMPLE 5: Backup Parallel Architecture (Reference SAE ARP4754, section 5.4.1.5, and RTCA DO-178B, section 2.2.3)

Safety Assessment	SAE ARP4754	RTCA DO-178B	RTCA DO-254
<p>An a/c level function is implemented in a parallel architecture in which a backup channel operates only after the primary channel fails, as described in SAE ARP4754, section 5.4.1.5.</p>  <p>Sa is the primary portion. Sb is the backup. Sa and Sb are independent.</p> <p>Suppose the safety assessment findings are as follow:</p> <p>FHA:</p> <ul style="list-style-type: none"> Effects of functional failures: <ul style="list-style-type: none"> Malfunction = Catastrophic Loss = Major Effect of Sa alone: Hazardous (malfunction) Effect of Sb alone: Minor (Loss) <p>PSSA:</p> <ul style="list-style-type: none"> Sa must meet integrity requirements without the backup and must have a very low hardware failure rate – less than 1×10^{-7} for loss of function – as discussed in paragraph 5.4.1.5. Sa to have higher DAL than Sb No hardware common mode failures. 	<p>Per item 5 in Table 4:</p> <p>The overall system is Level A.</p> <p>Sa is Level A, regardless of its hazardous effect. Sb can be Level C albeit its effect is Minor.</p> <p>Per Note 2 of the table, the switching, voting, fault detection is Level A.</p>	<p>The guidance for parallel architecture section 2.2.3 recommends the software in either to be at Level A. The other channel can be Level C corresponding to the <u>loss</u> of the aircraft level function (Major). The software that determines that the primary channel has failed (fault detection or safety monitoring) and switches to the backup channel would be Level A.</p>	<p>Using the same strategy as SAE ARP4754, the PSSA would assign Level A to the hardware of Sa and Level C to Sb.</p>

Summary

- Because the PSSA requires Sa to be Level A, the three guidance are consistent in their DAL assignments.

EXAMPLE 6: An Electronic System with Manual Safety Feature

Suppose an airplane has inherent lightly damped dutch roll characteristics. A yaw damper (YD) system is provided to arrest the dutch roll and to improve ride quality. However, the YD system is not critical because without it the dutch roll will eventually damp itself out. Suppose the airplane safety assessment is as follows:

Airplane Level FHA:

- *Sustained* oscillation at the dutch roll frequency is Catastrophic.
- Loss of yaw damping function is at most Major taking into account the inherent dutch roll damping characteristics.
- YD failed “hardover” is Major.

System Architecture:

Based on the above failure conditions, a system architecture is established such that the yaw damping function is provided by two *identical* yaw damper modules (YDM) each of which has a failure rate of 10^{-5} /flt-hr. Only one module is in control at any given time. The YDMs monitor each other and both shut down if there are erroneous outputs. System shutdown is annunciated in the flightdeck. A manual switch is provided in the flightdeck to shut down the YDMs in case of malfunction (the pilot is the safety “monitor”). The yaw damping function is implemented in software.

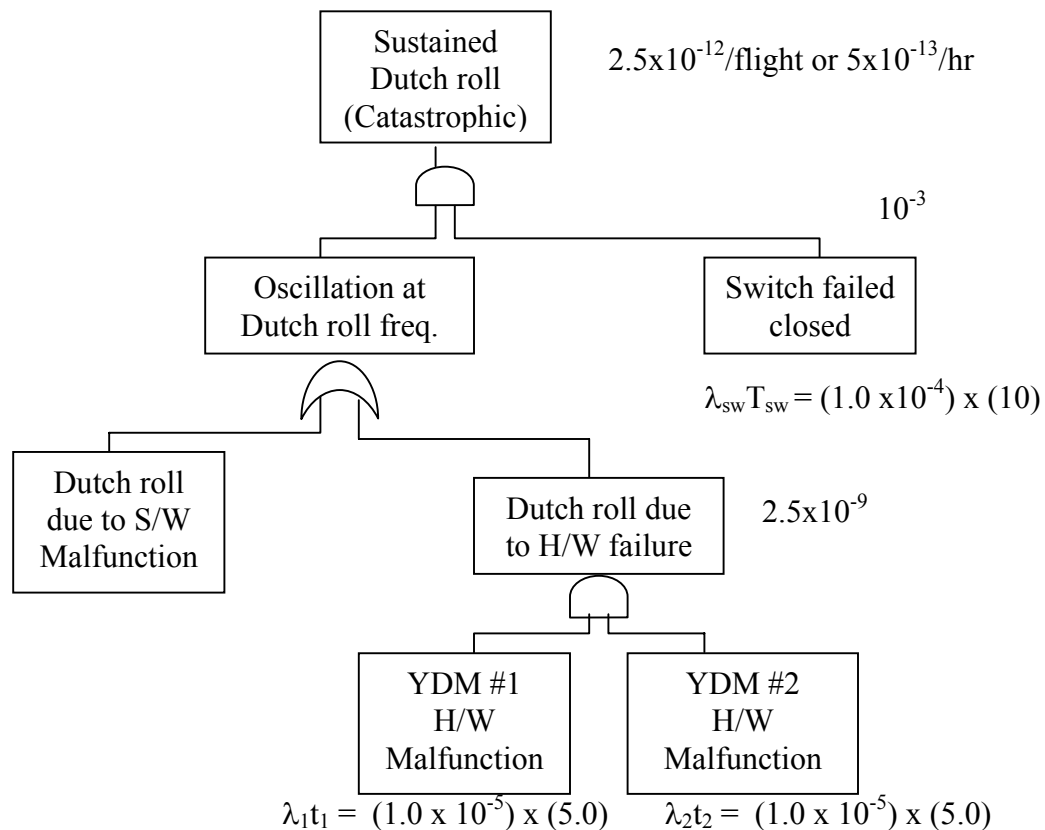
Suppose the system safety assessment produces the following results:

System Level FHA:

- YDM:
 - Loss of 1 YDM due to hardware failure is Major if it leads to shutdown of the good YDM.
 - Loss of 2 YDMs due to hardware failure is Major (loss of YD function).
 - Loss of YD function due to software is Major.
- Manual Switch:
 - Failed open is Major (causes loss of YD function)
 - Failed connected is Minor (slight reduction in system capability – loss of manual shutdown, no immediate safety effect on airplane)
 - The failure rate of the switch to the closed position is 1.0×10^{-4}
 - Establish a check of the manual switch every 10 flight hours

PSSA:

- For the switch failure to be Minor in the failed-connected condition, the two YDMs combined must be sufficiently reliable for the combination of malfunctioning YDM and switch failure to meet the numerical safety objectives (see fault tree below.)
- There are no common mode failures between the switch and the YDMs.
- Malfunction due to hardware common mode failure in both YDMs causing oscillation at dutch roll frequency is Hazardous (without the manual switch, this failure would be Catastrophic). It is assumed the pilot is trained to compensate by turning the YD switch to “Off”.
- Malfunction due to hardware failure in one YDM is Major.
- Software malfunction causing oscillation at dutch roll frequency is Hazardous (Catastrophic without the manual switch). It is assumed the pilot is trained to compensate by turning the YD switch to “Off”.
- Assume an average flight time of 5.0 hours

Fault Tree:**Development assurance Level Determination:**

- Using the SAE ARP4754 guidance:
 - The overall system (YDM and Switch) would be assured to Level A because the top hazard category is Catastrophic.

- YDM (as a system of s/w and h/w) is at Level B corresponding to the hazardous effect of a malfunction (assumed to occur simultaneously.)
- According to the FHA, the DAL of the switch should be Level B per 5.4.1.2. However, since the switch is a simple hardware component, no DAL is necessary and only the probability requirement needs to be satisfied.
- Software level according to RTAC DO-178B alone:
 - Because the top level effect is Catastrophic, the YD software is Level A albeit the system incorporates the manual safety switch.
- Hardware DAL according to RTCA DO-254:
 - Because the two YDMs have identical hardware, the safety assessment identifies the possibility of common mode failures. The YDM hardware are developed to Level B corresponding the Hazardous category due to both YDMs malfunctioning. If there were no common mode failures, the YDM could be Level C corresponding to the failure of each module.
 - No need for assigning DAL to the switch as it is a “simple” device.

Summary of DAL assignments for the Yaw Damper system:

Item	SAE ARP4754	RTCA DO-178B	RTCA DO-254
Overall system	A	-	-
YDM	B	-	-
-Software	B	A	-
-Hardware	B	-	B
Switch	-	-	-

Application of the policy would result in software Level B for the YDM taking into account the manual safety switch which is clearly independent and dissimilar from the YD modules.

EXAMPLE 7: A Mechanical System with Software Controlled Safety Feature

Suppose a mechanical air supply system duct must be routed in the vicinity of a fuel tank. If the duct bursts, the high temperature air could cause loss of structural integrity of the fuel tank, potentially leading to a catastrophic failure condition. To mitigate the effect, a monitoring system is used to detect the burst by sensing the high temperature and then direct the airflow away from the fuel tank vicinity.

Airplane Level FHA:

- Burst duct near the fuel tank and inability to isolate the duct failure is Catastrophic.
- Loss of monitoring function *alone* is Major (significant reduction in safety margin)

System Architecture:

Two identical and mutually independent monitors automatically drive an electrically operated isolation valve closed when a burst duct is detected (by temperature sensors.) The monitor system is dissimilar and independent from the duct system. The monitor channels employ software and “complex” electronic hardware. A duct burst condition is annunciated; however, the system does not rely upon flightcrew action to isolate the duct.

Suppose the system safety assessment produces the following results:

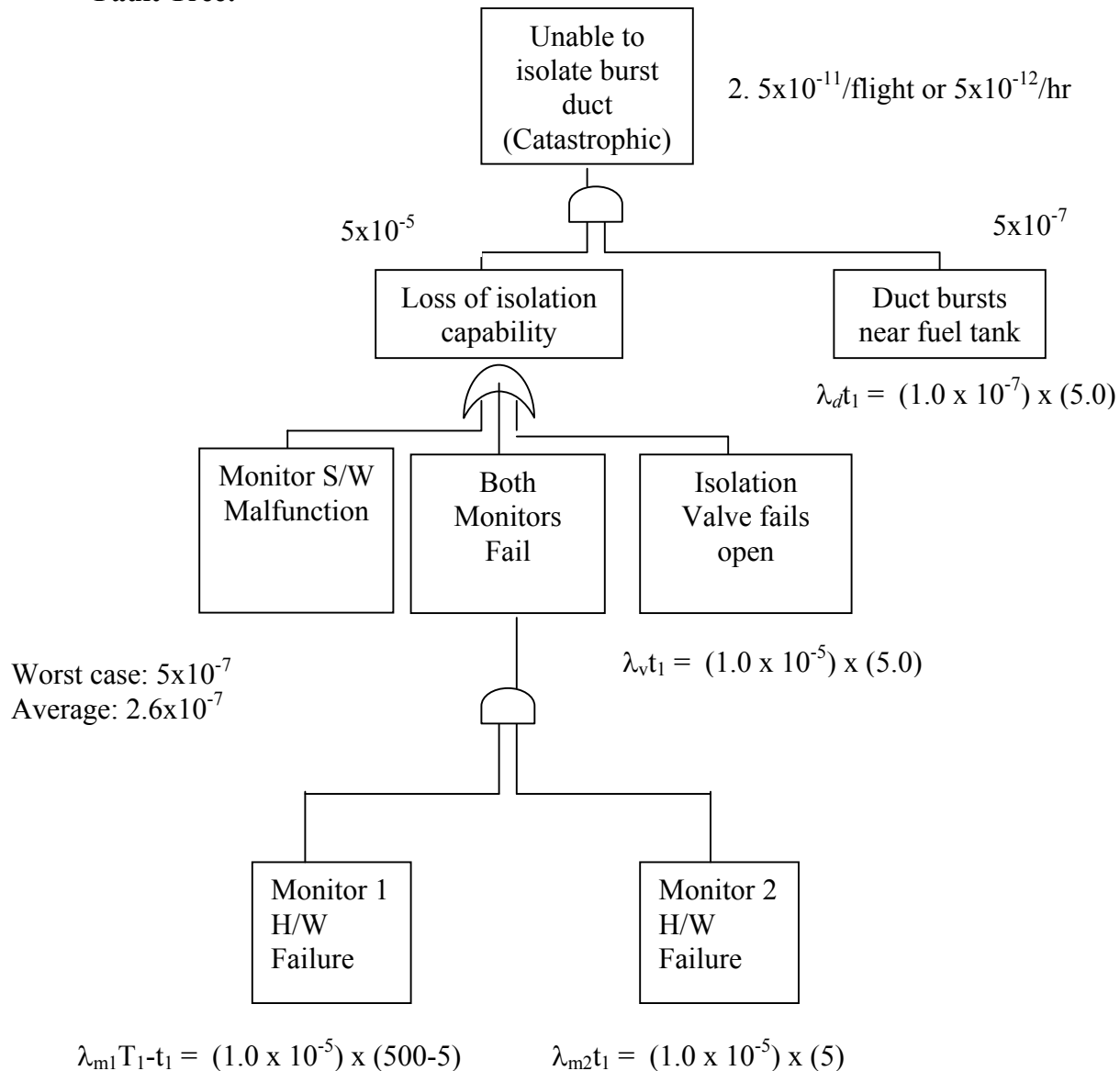
System Level FHA:

- Air duct failed = Major with the monitoring system functioning. The flightcrew is notified of the failure condition and will take appropriate actions to compensate for loss of the other systems that require air from the failed duct. Without the monitoring system (and automatic isolation of hot air,) this failure would be Catastrophic.
- Loss of both monitor channels due to a hardware failure is Major.
- Loss of 1 monitor channel due to a hardware failure is Minor as either channel can provide the monitoring and shutdown operations.
- Isolation valve fails open is Major (significant reduction in safety margin due to inability to isolate burst duct).
- Isolation valve fails closed is Minor (because of loss of systems served by the duct, there is an increase in crew workload to compensate for those losses.)

PSSA:

- Assume a flight time of 5 hours.
- Air supply duct burst failure rate is 10^{-7} flight-hour.
- Isolation valve failed-open rate is 10^{-5} per flight-hour and is not latent for more than 1 flight.
- Monitor channel failure rate is 10^{-5} per flight-hour.
- Software malfunction, assuming to happen to both channels simultaneously, causing loss of monitoring function is Major because of significant reduction in safety margin.
- Each channel is checked for proper operation every 500 flight hours.
- The duct system to have higher assurance level than its monitors.

Fault Tree:



Development assurance Level Determination:

- Using SAE ARP4754, the system level DALs are:
 - The overall system (duct + monitors) is Level A because the top hazard category is Catastrophic.
 - Using the guidance for active-monitor architecture, paragraph 5.4.1.4, the duct system is Level A, and the monitor is Level C, as specified by the PSSA. However, the duct system is composed of simple hardware components for which no DAL is necessary.
 - The isolation valve is a simple electromechanical device for which no DAL is necessary.

- The monitors are complex electronic devices with software that require a Level C DAL for both hardware and software.
- Software level using RTCA DO-178B:
 - Section 2.2.3 of RTCA DO-178B would assign Level A to the monitoring software.
- Hardware DAL using RTCA DO-254:
 - For this example, the strategy of SAE ARP4754 is used, so Level C is assigned to the monitor hardware.

Summary of DAL assignments:

Item	SAE ARP4754	RTCA DO-178B	RTCA DO-254
Overall system (duct system + monitoring system)	A	--	--
Duct system	A	--	--
Monitoring system	C	--	--
-Hardware	C	--	C
-Software	C	A	--

Application of the policy would result in Level C software for the monitors, provided that the duct system is developed to Level A.

DISTRIBUTION:

Manager, Aircraft Engineering Division, AIR-100
Manager, Boston Aircraft Certification Office, ANE-150
Manager, New York Aircraft Certification Office, ANE-170
Manager, Ft. Worth Airplane Certification Office, ASW-150
Manager, Ft. Worth Special Certification Office, ASW-190
Manager, Atlanta Aircraft Certification Office, ACE-115A
Manager, Wichita Aircraft Certification Office, ACE-115W
Manager, Chicago Aircraft Certification Office, ACE-115C
Manager, Anchorage Airplane Certification Office, ACE-115N
Manager, Seattle Aircraft Certification Office, ANM-100S
Manager, Los Angeles Aircraft Certification Office, ANM-100L
Manager, Denver Airplane Certification Office, ANM-100D
Manager, Brussels Aircraft Certification Office, AEU-100
Manager, Small Airplane Directorate, ACE-100
Manager, Rotorcraft Directorate, ASW-100,
Manager, Engine and Propeller Directorate, ANE-100